Title	On some generic expression of Gauss sums(Algebraic Number Theory)
Author(s)	Miki, Hiroo
Citation	数理解析研究所講究録 (1987), 603: 35-42
Issue Date	1987-01
URL	http://hdl.handle.net/2433/99659
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
603巻 1987年 35-42

On some generic expression of Gauss sums

By Hiroo Miki (三木 博雄)

Department of Mathematics, Tokyo Metropolitan University

§ Introduction.

Let ℓ be a fixed odd prime number and let ζ_{ℓ^n} be a primitive ℓ^n-th root of unity such that $\zeta_{\ell^{n+1}}^{\ell}=\zeta_{\ell^n}$ for $n=1,2,3,\cdots$. Put $K_n=\mathbb{Q}(\zeta_{\ell^n})$ for $n\geq 1$, where $\mathbb{Q}$ is the field of rational numbers. Let p be a prime number different from ℓ and let $\mathfrak{P}_n$ be a prime ideal of K_n for $n\geq 1$ satisfying

$$(p)\subset \mathfrak{P}_1 \subset \mathfrak{P}_2 \subset \cdots \subset \mathfrak{P}_n \subset \mathfrak{P}_{n+1} \subset \cdots .$$

We fix such a sequence of prime ideals. Let

$$\chi_{\mathfrak{P}_n}(x \bmod \mathfrak{P}_n) = \chi_n(x \bmod \mathfrak{P}_n) = \left(\frac{x}{\mathfrak{P}_n}\right)$$

be the ℓ^n-th power residue symbol in K_n for $x\in \mathbb{Z}[\zeta_{\ell^n}]$, where $\mathbb{Z}$ is the ring of rational integers. If $x\notin \mathfrak{P}_n$, then $\chi_n(x \bmod \mathfrak{P}_n)$ is the unique ℓ^n-th root of unity satisfying the congruence

$$\chi_n(x \bmod \mathfrak{P}_n) \equiv x^{(N\mathfrak{P}_n-1)/\ell^n} \pmod{\mathfrak{P}_n},$$

where $N\mathfrak{P}_n$ is the absolute norm of $\mathfrak{P}_n$. If $x \in \mathfrak{P}_n$, then $\chi_n(0)=0$.

Now we state the definition of Gauss sums and Jacobi sums. Put $\psi_n(x)=\zeta_p^{T_n(x)}$ for $x \in \mathbb{Z}[\zeta_{\ell^n}]/\mathfrak{P}_n$, where $T_n: \mathbb{Z}[\zeta_{\ell^n}]/\mathfrak{P}_n \to \mathbb{F}_p$ (the field of p elements) is the trace map.

Definition. For $a \in \mathbb{Z}$, put

$$g(\chi_n^a)=g_n(a)=g_{\ell^n}(\mathfrak{P}_n,a)= - \sum_{x \in \mathbb{Z}[\zeta_{\ell^n}]/\mathfrak{P}_n} \chi_{\mathfrak{P}_n}^a(x)\psi_n(x).$$

The sum is called a Gauss sum.

Definition. For $a, b \in \mathbb{Z}$, put

$$J_{\ell^n}^{(a,b)}(\mathfrak{P}_n) = - \sum_{\substack{x,y \in \mathbb{Z}[\zeta_{\ell^n}]/\mathfrak{P}_n \\ x+y=-1}} \chi_{\mathfrak{P}_n}^a(x)\, \chi_{\mathfrak{P}_n}^b(y) .$$

The sum is called a Jacobi sum.

As is well known, Gauss sums and Jacobi sums have close relation to each other; the Jacobi sum can be expressed in terms of Gauss sums in the following:

$$J_{\ell^n}^{(a,b)}(\mathfrak{P}_n) = (N\mathfrak{P}_n)^{-1} g_{\ell^n}(\mathfrak{P}_n,a) g_{\ell^n}(\mathfrak{P}_n,b) g_{\ell^n}(\mathfrak{P}_n,c),$$

where $a+b+c \equiv 0 \pmod{\ell^n}$ and $(a,b,c) \not\equiv (0,0,0) \pmod{\ell^n}$.

Recently, Y.Ihara ([7],Theorem 7) found a power series which

interpolates $J_{\ell^n}^{(a,b)}(\wp_n)$ with $n=1,2,3,\cdots$. Put

$$\Lambda = \mathbb{Z}_\ell[[u,v,w]]/((1+u)(1+v)(1+w)-1) \cong \mathbb{Z}_\ell[[u,v]],$$

where $\mathbb{Z}_\ell[[u,v,w]]$ is the formal power series ring in three variables u, v and w over the ring of ℓ-adic integers $\mathbb{Z}_\ell$.

Theorem ([7],Theorem 7). There exists a power series $F_p(u,v,w)\in\Lambda$ satisfying

$$J_{\ell^n}^{(a,b)}(\wp_n) = \prod_{i=0}^{f_n-1} F_p(\zeta_{\ell^n}^{ap^i}-1, \zeta_{\ell^n}^{bp^i}-1, \zeta_{\ell^n}^{cp^i}-1)$$

for all $a,b,c\in\mathbb{Z}$ such that $(a,b,c)\not\equiv(0,0,0) \pmod{\ell}$ and $a+b+c \equiv 0 \pmod{\ell^n}$, and for all $n\geq 1$. Here f_n is the order of p in $(\mathbb{Z}/\ell^n)^\times$.

Note that Ihara([7],Theorem 7) gives a more general result than the above statement.

For the proof, Ihara [7] uses the ℓ-adic Tate module of the Jacobian variety of the Fermat curve of degree ℓ^n in the limit as $n\to\infty$, and studies its Galois module structure; the module is a free Λ-module of rank 1 and the action of Frobenius over p on the module corresponds to the above Ihara's power series $F_p(u,v,w)$.

At the Kyoto conference Oct.1985, G. Anderson stated that he found a power series of one variable interpolating Gauss sums into which Ihara's power series can be factored (see [1]). Using Deligne's

theory [5] on absolute Hodge cycles, he developes the theory of hyperadelic gamma functions and beta functions, and relates Ihara's power series to Anderson's adelic beta function.

In the present paper, we shall consider the following purely local problem.

Problem(purely local). For a given sequence of local ℓ-units $u_1, u_2, \cdots, u_n, \cdots$, find a necessary and sufficient condition for $u_1, u_2, \cdots, u_n, \cdots$ to be interpolated as in the above Ihara's Theorem.

In the following, we shall give a partial answer to the problem and obtain another proof of the special case of Anderson's result.

§1 Interpolation of local units in $\mathbb{Q}_\ell(\zeta_p)$.

Put $K_i' = \mathbb{Q}_\ell(\zeta_{p\ell^i})$ for $i=1,2,3,\cdots$, where $\mathbb{Q}_\ell$ is the field of ℓ-adic numbers.

Theorem 1. Let $u_1, u_2, \cdots, u_n, \cdots$ be a sequence of principal units of K_1'. Then there exists a power series $F(T) \in \mathbb{Z}[\zeta_p][[T]]$, $F(T) \equiv 1 \pmod{T}$, satisfying $N_{K_i'/K_1'}(F(\zeta_{\ell^i}-1)) = u_i$ for all $i \geq 1$, if and only if the following two conditions (i) and (ii) are satisfied for all $i \geq 1$.

(i) $N_{K_1'/\mathbb{Q}_\ell}(u_i) \equiv 1 \pmod{\ell^i}$.

(ii) $u_{i+1} \equiv u_i^{\tau} \pmod{\ell^i}$, where $\tau \in G(\mathbb{Q}_\ell(\zeta_{\ell^\infty p})/\mathbb{Q}_\ell(\zeta_{\ell^\infty}))$ is the Frobenius automorphism.

The proof is rather complicated and technical. We use local class field theory and the analysis of elements of norm 1, in particular, Hasse's classical result on the relation between the norms and the Hasse function (cf. e.g. Serre [14]), but we do not use algebraic geometry.

We also note that the above Theorem 1 has a similarity to the Coleman power series [2](see also Theorem 13.38 of Washington [16]).

§2 Congruence for Gauss sums.

Let $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}}_\ell$) be an algebraic closure of $\mathbb{Q}$ (resp. $\mathbb{Q}_\ell$). By a fixed imbedding, we consider $\overline{\mathbb{Q}}$ as a subfield of $\overline{\mathbb{Q}}_\ell$.

Theorem 2. Let M be the decomposition field of p in $\mathbb{Q}(\zeta_{\ell^\infty p})/\mathbb{Q}(\zeta_p)$ and let $\mathcal{O}_{M\mathbb{Q}_\ell}$ be the ring of integers of $M\mathbb{Q}_\ell$. Let τ be as in Theorem 1. Then the following (i),(ii) and (iii) hold for all $i \geq 1$.

(i) $g(\chi_i^a) \in M$.

(ii) $g(\chi_{i+1}^a) \equiv g(\chi_i^a)^{\tau} \pmod{[\mathbb{Q}(\zeta_{\ell^{i+1}p})M:M]\mathcal{O}_{M\mathbb{Q}_\ell}}$.

(iii) $N_{M\mathbb{Q}_\ell/\mathbb{Q}_\ell}(g(\chi_i^a)) \equiv 1 \pmod{\ell^i\mathbb{Z}_\ell}$.

§3 Interpolation of Gauss sums.

As an application of Theorems 1 and 2, we obtain another proof of the special case of Anderson's result([1]).

Theorem 3. Assume $\ell \,||\, (p-1)$, i.e., the exact power of ℓ dividing $(p-1)$ is ℓ. Then there exists a power series $F(T) \in \mathbb{Z}_\ell[\zeta_p][[T]]$ satisfying the following (i) and (ii):

(i) $F(T) \equiv 1 \pmod{T}$.

(ii) $g(\chi_n^a) = \prod_{i=0}^{f_n-1} F(\zeta_n^{ap^i}-1)$ for all $a \not\equiv 0 \pmod{\ell}$ and for all $n \geq 1$, where f_n $(=\ell^{n-1})$ is the order of $p \bmod \ell^n$ in $(\mathbb{Z}/\ell^n)^\times$.

References

[1] G. Anderson, The hyperadelic gamma function: a précis, to appear in Advanced Studies in Pure Math., Vol.12.

[2] R. Coleman, Division values in local fields, Invent. Math. 53(1979),91-116.

[3] R. Coleman, "Applications" of Ihara's power series to cyclotomic fields, a lecture at Univ. Tokyo in Oct. 1985.

[4] P.Deligne, Applications de la formule des traces aux sommes trigonométriques, Sém. Géom. Alg. SGA 4½, Cohomologie Etale, Lecture Notes in Math. 569,pp.168-232, Springer, Berlin Heidelberg New York 1977.

[5] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, Proc. Symp. Pure Math. AMS 33(1979), part 2, 313-346.

[6] R. Greenberg, On the Jacobian variety of some algebraic curves, Compositio Math. 42(1981), 345-359.

[7] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. 123(1986), 43-106.

[8] Y. Ihara, M. Kaneko and A. Yukinari, On some properties of the universal power series for Jacobi sums, to appear in Advanced Studies in Pure Math., Vol. 12.

[9] Y. Ihara, On Galois representations arising from towers of coverings of $\mathbb{P}^1\setminus\{0,1,\infty\}$, General constructions, Preprint.

[10] K. Iwasawa, A note on Jacobi sums, Symposia Math. 15 (1975), 447-459.

[11] K. Iwasawa, A note on cyclotomic fields, Invent. Math. 36 (1976), 115-123.

[12] H.Miki, On the ℓ-adic expansion of certain Gauss sums and its applications, to appear in Advanced Studies in Pure Math. Vol. 12.

[13] H. Miki, On the congruence for Jacobi sums and its application

to Weil's Grössencharacter, in preparation.

[14] J.-P. Serre, Corps locaux, 2-nd edition, Hermann, Paris,1968. = Local Fields, GTM 67, Springer, New York Heidelberg Berlin, 1979.

[15] T. Uehara, On cyclotomic units connected with p-adic characters, J. Math. Soc. Japan 37(1985), 65-77.

[16] L.Washington, Introduction to Cyclotomic Fields, GTM 83, New York Heidelberg Berlin, 1982.

[17] A. Weil, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949), 497-508.

[18] A. Weil, Jacobi sums as "Grossencharaktere", Trans. Amer. Math. Soc. 73 (1952), 487-495.

[19] A. Weil, Sommes de Jacobi et caractères de Hecke. Gött.Nachr. 1974,Nr.1,14pp.

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan